INTRODUCTION

The continuous adoption of emerging technologies by the government, public, and private sectors to conduct business has influenced many other sectors, including educational institutes to move their operations online. This caused the higher education to move and expand their teaching modality and services and the trend toward online services. The new trend imposes institutes' administrations to allow their community members (faculty, students, and staff) utilizing their mobile devices in addition to standard computer devices to do their work. Additionally, it provides relatively open access to its community members and the public off-campus communities (parents, alumni, and cooperating industries).

The increase of such movement leads to increase number of victims to different types of attacks and the number of cybercrimes. There are variety of reasons for the increase of information security incidences including but not limited to electronic data, mobile devices, and lack of information technology (IT) security knowledge among Internet users. “The users are the weakest link which hackers use to break into an organization” (Katz, 2005). Unintentional mistakes caused by the users such as downloading unknown-source attachments are considered one of the top threats to information security in an organization (Whitman & Mattord, 2012). Therefore, a program such as Information Security Education, Training, and Awareness program that continuously educating professionals and users how to utilize the new and advanced security technology is indeed in dire need. Hereafter, the acronym “InfoSec” in this paper will refer to any Information Security program including Education, Training, and Awareness programs.

Despite the availability of the information security technology and official organization standards, a high percentage of higher education institutes offer no InfoSec to their professionals and users. Referring to Marks and Rezgui (2009), only third of the surveyed 435 higher education institutions had a complete or partial InfoSec program. Androulidakis and Kandus (2011) stated that 66% of higher education institutes reported that they have no formal InfoSec program for their community members.

InfoSec program plays a significant role in the process of the overall information security system and should be offered by higher education institutions. Pressure toward having this program in place is likely to come from faculty and the student body, which increasingly handling mobile devices and using them as support tools to their
course work-study. Therefore, initiating and implement- ing an InfoSec program in higher education environment becomes a must and crucial.

The remaining of this paper is constructed in 8 sections. Section two discusses InfoSec program background. Section three, presents the literature review of the Info- Sec program. Section four describes the methodology employed in this research. Section five discusses the data analysis and research findings. Section six highlights the importance of the administrators' roles. Conclusion and recommendations are elaborated in section seven. Finally, limitations of the study and future research are discussed and proposed in section eight.

INFORMATION SECURITY PROGRAM BACKGROUND

InfoSec program enhances educational and training pro- grams by focusing on information security. The purpose of InfoSec is to enhance security in three ways: first, build- ing in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and sys- tems. Second, developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely. Third, improving awareness of the need to protect system resources (Whitman & Mattord, 2012). The following subsections present a brief descrip- tion to the three components of the InfoSec program.

Security education

Security Education is defined in National Institute of Standards and Technology (NIST) Special Publication 800-16 as follows: 'The Education level integrates all of the security skills and competencies of the various func- tional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and princi- ples (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.” (as cited in Wilson & Hash, 2005, p. 9)

Security Training

The component of security training in the InfoSec pro- gram trains employees to be equipped with the needed security skills in a manner controlling risks that may threaten organizations' resources and users. End-user security training component is quickly becoming an in- tegral part of every organization, in particular the large ones (Vacca, 2009; Herold, 2010). An organization may spend millions of dollars securing their networks, hiring consultants, and hardening their systems. However, with- out proper security training of the authorized users, these efforts will be futile.

Several methodologies including traditional face-to-face, computer-based, online, and a combination of both (face- face, and computer based) can be used to conduct a secu- rity training program. Regardless the deployed methodol- ogy, security training program is only effective if trainees are able to retain what they have learned and gathered (Herold, 2010).

Security Awareness

Security awareness is designed to modify any person be- havior that endangers the security of the organization’s information. It keeps information security at the fore- front of users' minds on a daily basis (Kritzinger & Smith, 2008). Therefore, it installs a sense of responsibility, which leads users to care more on how to use their devices, what type of information to exchange, and what type of data and information to store in it. Moreover, it minimizes the risk of accidental compromise, damage, or destruction of information. Despite being an effective security method, the concept of security awareness is the least frequently implemented as noted in NIST Sp800-12 (Guirman & Roback, 1995).

Many security awareness components are available at low costs, or virtually no cost except paying for the time and energy of the developer while others can be expensive (An- droulidakis & Papapetrou, 2008). A security awareness program can deliver its message via videotapes, newsletter, posters, bulletins, boards, flyers, demonstrations, brief- ings, talks, lectures, or short reminder notice at logon. An organization can establish a webpage or a site dedicated to promoting information security awareness such as the capability of informing the employees via email when infor- mation related to security is posted.

Effective security awareness programs need to be designed with the recognition that tends to practice a tuning out process. For instance, a security poster will be ignored and blended into the environment regardless of how well it is designed. For this reason, awareness techniques should be creative and frequently updated (Guirman & Roback, 1995; Whitman & Mattord, 2014).

LITERATURE REVIEW

Emerging technologies including mobile devices are be- coming an essential element of a higher education envi- ronment. A mobile device is an efficient communication device that is an integral part of daily life for billions of people around the world. Regardless the purpose of their use, educational, personal, for entertainment or business, the mobile devices have contributed to the escalated growth of the m-education (Traxler, 2007).

The use of mobile technologies can overcome the limita- tion of educational flexibility with wired technology. The advantages of mobility and mobile wireless technolo- gies help improve efficiency and effectiveness of teaching and learning process (Ally, 2009), but at the same time, it raised many challenges particularly the security issues which would be suppressed by deploying the InfoSec pro- gram. Thomson and Solms (1998) reported that InfoSec program plays a significant role in the process of strengthening the overall information security posture of education organizations, especially in the context of higher education environments. Accord- ing to Katz (2005) and Eyadat (2015) there is a need for promoting information security standards and practices within an organization and they proposed that all users should be aware of disciplinary actions resulting from non-compliance with the organization's information se- curity procedures. A successful organizational informa- tion security policy should incorporate clear definitions of user responsibilities for information security (Gaunt, 2000; Whitman & Mattord, 2014). Similarly, Banerjee, Cronan, and Jones (1998) reported that organizations should introduce information security awareness and make their ethical policy clear to their employees and ensure that strong deterrents are in place. As an informa- tion security professional, the researcher strongly believes these could be achieved through implementing InfoSec program in an organization’s information systems.

METHODOLOGY

Fifty-nine websites of higher education institutes in Saudi Arabia were examined to understand the types and the ex- tent of the InfoSec program included on the institute web- sites. Using two different browsers, Internet Explorer and
Google Chrome, each site of the institute was surfed three to five times during the research period in 2013. Updates on the InfoSec program of the examined institute sites were recorded through the repetitive visitations.

Information security professionals and managers from one of the examined institutes were contacted and invited for face-to-face interview following the preliminary website results. Based on their availability, a group of 8 professionals was non-randomly selected and interviewed for their insights on the involvement of the administrators and on the level of InfoSec program implementation. Interview questions were adopted and modified from NIST 800-50 (Wilson & Hash, 2005) to reflect the initial findings from the preliminary website results.

DATA ANALYSES AND RESULTS
Quantitative data analysis was conducted on the data collected from 59 Saudi Arabian Institute websites as well as the interview data collected from the information security professional staff worked in one of the surveyed institutes.

WEBSITE DATA ANALYSIS
From the examined 59 Saudi Arabian Institute websites, 32 were recorded as having neither complete nor partial information security program in place as shown in Table 1 and figure1. This translates into more than half (54%) of the institutes examined were at high risk and vulnerable to the information security attacks. Tremendous efforts of convincing the top management administrators to put InfoSec program in place should be seriously considered by the information security professionals and managers to protect the resources and assets of the institutes.

### Table 1: Security Program Adoption in 59 Saudi Arabian Institutes

<table>
<thead>
<tr>
<th>Components Deployed</th>
<th>Number of Institutes</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, or 3 Components</td>
<td>27</td>
<td>46%</td>
</tr>
<tr>
<td>none of the Components</td>
<td>32</td>
<td>54%</td>
</tr>
</tbody>
</table>

Frequency and relative frequency of the adoption of the individual category of the InfoSec program, namely, security education, security training, and security awareness, from the 59 institute websites examined were displayed in Table 2 and Figure 2.

Twenty-Seven institutes deployed one or more of three components (Table1, Figure1). Of the Twenty-Seven institutes having InfoSec program in place, 26 of them have either a complete or a partial awareness component implemented. (Tables 2). Seventeen of them only had the three components implemented, namely, security education, training, and awareness (table3). The remaining 10 institutes, one of them implemented only one component, namely, training security program. The other 9 institutes implemented only the awareness security program (Table 4). The results reflect deficient attention in regard to the security awareness, training, and education. The importance of implementation of the InfoSec program is urgent for suppressing the potential vulnerability to the internal and external threats.

### INTERVIEW DATA ANALYSIS
Based on the findings from the preliminary websites examination, five questions were asked during each interview to solicit the interviewee's opinions in regard to the causes of inadequate implementation of the InfoSec program. Specifically, the interview questions were:

1. What are the most critical issues facing information security executives to implementing InfoSec program?
2. What is the impact of absence of InfoSec program in raising security issues among your campus community members?
3. How much agreement is there between the information security professionals and the top management administrators about the importance of deploying InfoSec programs?
4. Did you have formal training in information and system security? Have employees received adequate training to fulfill their security responsibilities?
5. What is the impact of the cultural practices on the success of information security program?

![Table 2: Individual Deployed Component](image1)

<table>
<thead>
<tr>
<th>Number of Institutes</th>
<th>Education</th>
<th>Training</th>
<th>Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>59</td>
<td>Yes 17</td>
<td>No 42</td>
<td>Yes 33</td>
</tr>
<tr>
<td></td>
<td>No 41</td>
<td></td>
<td>No 26</td>
</tr>
</tbody>
</table>

![Table 3: Categories Deployed By Component](image2)

<table>
<thead>
<tr>
<th>Number of Components Deployed</th>
<th>Number of Institutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>1</td>
<td>27</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

![Table 4: Distribution of the Deployed Individual Component](image3)

<table>
<thead>
<tr>
<th>Components Deployed</th>
<th>Number of Institutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education, Training, &amp; Awareness</td>
<td>17</td>
</tr>
<tr>
<td>Training only</td>
<td>1</td>
</tr>
<tr>
<td>Awareness only</td>
<td>9</td>
</tr>
<tr>
<td>Total</td>
<td>27</td>
</tr>
</tbody>
</table>

![Figure 2: Individual Deployed Component](image4)
The responses of the interviews showed the top three main reasons for lacking the InfoSec program in place. Among the top three main reasons, 94% of the participants revealed insufficient level of knowledge and practices in the InfoSec program of information security and IT staff that qualified them to conduct in-house training or initiated an effective awareness program. Followed by 91% of the interviewees agreed that staff and management managers' support will play a focal factor in initiating a project which is caused by the lack of protection. Furthermore, the interviewees resisted changes, in particular, related to information technologies, software, tools, and policies. Finally, 81% of the interviews revealed that there was no support from the top management administrators to initiate InfoSec program.

Although the issues of insufficient knowledge, resistance of change from the staff members, and lacking administers’ support were challenges faced among the interviewees examined, almost all (98%) of the interviewees stated that it was vital and urgent to deploy the InfoSec program immediately to prevent potential vulnerability caused by the lack of protection. Furthermore, the interviewees unanimously agreed that the top management administrators’ support will play a focal factor in initiating a standard for having InfoSec program in place.

NEED FOR ADMINISTRATORS SUPPORT AND OVERSEE

Higher Education Institutes are adopting InfoSec program to reduce risks that caused by having too many users connected to the same network including students, faculty, staff, administrative, alumni, parents, and community members. For example the majority of organizations in their websites show information on policies and guidelines in order to prevent phishing, malware, virus alerts, and potential other computer security awareness information which contain with specific guidelines that align with the organizations’ missions and goals. This approach facilitates the way of utilizing organization resources for all types of users and reduces potential internal and external related security incidents. In turn it will save resources, reduce carry cost, and utilize working time which in turn they are significant factors for improvement of organizational performance (Reinhart, R. (2014)).

Having a workforce that is educated and more aware of security areas is like expanding the Information Security department into the whole company. Also it gives the security managers a broader base of brainpower in which they can tap if needed. In other words, instead of having a group of staff trying to secure a specific organization’s asset against internal and external threats, it has everyone in the organization looking out for the security interests of the organization. Stephanie D. Hight (2005), stated that if an organization can make people aware of their surroundings, both physically and electronically, it can help the organization to defend against the known and hidden threats.

It is very common for organizations to underestimate the consequences of security transgression specially on today’s organizations that involve online transaction via mobile devices and wireless connections. Therefore, many organizations require high standards in employee’s training and education, also they implement and strictly enforce policies that help protect organization’s information (Vacc, 2009; Eyadat, 2015). Administrators should acknowledge that employees are the first line of defense in the organization since they have an access to the most crucial company information and systems and know how to distinguish between normal patterns and unusual activity. Consequently, no one is better suited to protect company information, than they are; therefore, their training and awareness should be the main focus when it comes to information security.

The great effort of the administrators in deploying InfoSec program will empower the top level management to best utilize and save invaluable resources including time and money. Also it improves the ability of the employees to acquire the required knowledge, skills, and awareness to properly perform their tasks which is vital for an organization to be competitive and enhance its performance (Vacc, 2009).

In summary, top management administrators should support and work together with the information security professionals to assure that a successful InfoSec program is in place. Moreover, administrators should stress the idea of integrating InfoSec into their strategic manage model, so to be more effective and then enhance organizational information management and performance.

CONCLUSION AND RECOMMENDATIONS

The security of institute information systems could be enhanced through InfoSec, specifically, education and training on the issues of security lead to improvement of security awareness. The increase of the knowledge on security issues provides a better practices to the institute’s community members, which in turn protects the system resources.

This research highlighted the importance of the administrators’ roles in deploying InfoSec program and examined the current status of the InfoSec program employed by the Saudi Arabian higher education institutes. The research also discovered an alarming and troublesome low rate of having InfoSec program in place. The results indicate that 81% of the interviewees revealed that there was no support from the top management administrators to initiate a partial or full InfoSec program this led to the other finding which is a high percentage (56%) of the examined institutes offer no InfoSec program and only 44% offer a low level of InfoSec program. The results are also discovered an alarming and troublesome low rate of having InfoSec program in place.

The study focused on one country and this may limit its generalization. Therefore, by including other institutes from different countries and in the same region. This could reflect different InfoSec programs’ status. Personal interviews could be increased to include administrators from different levels and different institutes. This could have added valuable data to lead to greater insight into the participants’ thoughts and opinions. A standard framework for an effective InfoSec program that aligns with the religion, culture, and regulation of that region could be established through further research.

REFERENCES


Androulidakis, I., & Kandus, G. (2011). What university students do (or don’t) know about security in their mobile phones. Telfor Journal, 3(1).


What is HPT: http://www.ispi.org/content.aspx?id=54 , (Viewed Number 2014)


